

Uncommon information (the cost of exchanging a quantum state)

Jonathan Oppenheim

Department of Applied Mathematics and Theoretical Physics, University of Cambridge U.K.

Andreas Winter

Department of Mathematics, University of Bristol, Bristol BS8 1TW, U.K.

If two parties share an unknown quantum state, one can ask how much quantum communication is needed for party A to send her share to party B . Recently, it was found that the number of qubits which should be sent is given by the conditional entropy. This quantifies the notion of partial information, and it can even be negative. Here, we not only demand that A send her state to B , but additionally, B should send his state to A . Paradoxically, we find that requiring that the parties perform this additional task can lower the amount of quantum communication required. This primitive, which we call *quantum state exchange*, can be used to quantify the notion of *uncommon information*, since the two parties only need to send each other the parts of their state they don't hold in common. In the classical case, the concept of uncommon information follows trivially from the concept of partial information. We find that for quantum states, this is not so. We prove upper and lower bounds for the uncommon information and find optimal protocols for several classes of states.

We now understand information in operational terms. We quantify it in terms of the amount of communication required to convey messages. For classical messages represented by a probabilistic source producing messages X Shannon showed that a rate of $H(X)$ bits are required to convey the message, where $H(X) = -\sum p_x \log_2 p_x$ is the Shannon entropy [1]. Likewise, for a source producing unknown quantum states with density matrix ρ_A , Schumacher [2] showed that $S(A)$ quantum bits (qubits) are necessary and sufficient to send the states where $S(A) = -\text{Tr} \rho_A \log \rho_A$ is the von Neumann entropy and we drop the explicit dependence on ρ . We thus see that the operational notion of information corresponds to calculable quantities.

Now, if the receiver has some prior information about the messages to be sent, then generally, less bits (or qubits) need to be sent. If we represent the receiver's prior information by the variable Y , then the Slepian-Wolf theorem [3] tells us that $H(X|Y) = H(XY) - H(Y)$ bits will convey the message. This quantity is called the conditional entropy, and it gives us a notion of how much *partial information* needs to be sent if the receiver has some prior information. The quantum counter-part of partial information was recently found by Horodecki and ourselves, [4, 5] through considering an analogous scenario we called *quantum state merging*. Instead of sharing a random variable XY , two parties (named Alice and Bob), share unknown states from an unknown ensemble with density matrix ρ_{AB} . We then allow free classical communication, and ask how many qubits Alice needs to send so that Bob receives her state. This quantifies the partial quantum information, and it was shown to be $S(A|B) = S(AB) - S(B)$, the quantum conditional entropy. Such a quantity was known previously, and it had been observed that it can be negative for entangled states [6, 7, 8]. State-merging shows that it has a meaning in

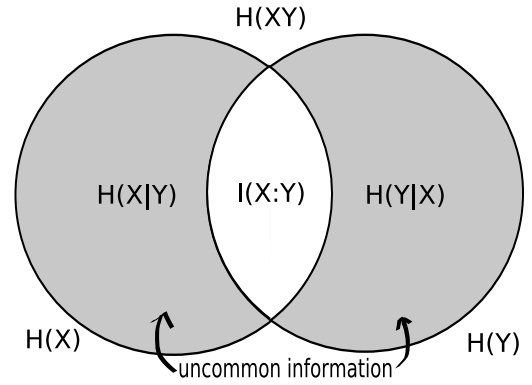


FIG. 1: A graphical representation of the uncommon information (shaded area) in classical information theory. The total information of the source producing pairs of random variables X, Y is $H(XY)$, while the information contained in just variable X (Y) is $H(X)$ ($H(Y)$). The information common to both variables is the mutual information $I(X : Y)$ (unshaded), while the partial informations are the conditional entropies $H(X|Y)$ and $H(Y|X)$. In the quantum case, the quantum mutual information $I(A : B)$ can be greater than the total information $S(AB)$. To compensate, the partial informations $S(A|B)$ and $S(B|A)$ can be negative. As we show, the uncommon information, defined operationally as state-exchange, must be positive in the quantum case. It thus cannot be the sum of the two partial informations and can not appear on this diagram.

terms of information. The fact that it can be negative then becomes natural – the conditional entropy quantifies how many qubits need to be sent from Alice to Bob, and if it is negative, Alice and Bob gain the potential to send future quantum states at no cost. Alice can not only send her state to Bob, but the parties are additionally left with maximally entangled states which can be used in the future to teleport quantum states without

using a quantum channel.

Finally, in classical information theory, there is the notion of *mutual information* – the amount of correlation between two variables. This is given by $I(X : Y) = H(X) + H(Y) - H(XY)$, which has the operational meaning as the rate at which messages can be reliably sent through a channel which takes X to Y (after maximizing $I(X : Y)$ over inputs) [1]. The building blocks of classical information can thus be represented by the Venn diagram of Figure 1. We will see that in quantum information theory, the Venn diagram is completely inadequate for representing the basic building blocks of the theory, and in fact, even entropies appear inadequate. Already, the analogous quantity for the mutual information is slightly less clear. One analogous task is the sending of quantum states through a noisy quantum channel, which can be done at a rate equal to a quantity called the coherent information $I(A|B) = S(B) - S(AB)$. This quantity is asymmetric unlike the quantum mutual information $I(A : B) = S(A) + S(B) - S(AB)$ (which can also be seen as a measure of total correlations – both classical and quantum [10]). Other quantities which might be seen as giving meaning to the notion of shared (common) correlations in quantum states including the entanglement cost E_c and the distillable entanglement D (how many maximally entangled states are required to create a shared state or are obtainable from it). The last one is a natural measure of pure quantum common information as classical communication is taken to be free for this task.

Here, we consider a concept which is complementary to the mutual information – we thus call it the *uncommon information* (since mutual information is sometimes referred to as *common information*). In the classical case, we can quantify it by considering two parties, and ask how much classical communication is required for them to exchange their messages. I.e. if Alice has X and Bob Y , how much communication do they need for Bob to get X and Alice to get Y . This naturally and operationally defines the notion of uncommon information, since they will have to transfer to each other the parts of their message which the other party doesn't know about. It is also a common communication primitive – most conversations involve exchanging information. The solution to this problem follows immediately by application of the Slepian-Wolf theorem – Alice sends $H(X|Y)$ bits to Bob, who then has X , and Bob then sends $H(Y|X)$ bits to Alice so that she has Y . This nicely divides the total information $H(XY)$ into two parts, the mutual information $I(X : Y)$, and the uncommon information $U(X : Y) \equiv H(X|Y) + H(Y|X)$. We then see that $S(XY) = I(X : Y) + U(X : Y)$.

We now want to find the appropriate quantum counterpart to the classical uncommon information. As we did with state merging, we will consider an operational task which is analogous to the classical task – we call it *quantum state exchange*. Namely, Alice and Bob share

unknown states which are emitted from a source characterized by density matrix ρ_{AB} – they want to swap states, and we ask how many qubits they need to send in total, while allowing classical communication for free (since we are interested in isolating the quantum part of the information). Also consider the case. Unlike the classical case, where the Slepian-Wolf theorem allows one to quickly solve message exchange, we will see that one cannot use state merging to solve this problem – the situation is completely different. Indeed this must be so – the quantity $S(A|B) + S(B|A)$ can be negative, and if it gave the rate for state exchange, Alice and Bob would be able to continually exchange their states, generating an arbitrarily large amount of pure entanglement. In essence we will see that, quantum state merging does not solve the problem of state exchange due to the no-cloning theorem [11]. $S(A|B) + S(B|A)$ thus appears to have no physical or operational information-theoretic meaning – in sharp contrast to the classical case.

In the remainder of this article, we will more formally define the notion of quantum state exchange, and then provide several protocols and solve some examples. We then provide an upper bound for the quantum uncommon information $\Upsilon(A : B)$ given by $E_c(R : A) + E_c(R : B)$ where the system R purifies ρ_{AB} , i.e. there is a pure state $|\psi\rangle_{ABR}$ and $\text{Tr}_R|\psi\rangle\langle\psi|_{ABR} = \rho_{AB}$. $S(AB)$ is also proven to be an upper bound. E_c is the amount of pure state entanglement needed to create a state between two parties [12, 13]. We shall then prove a lower bound on $\Upsilon(A : B)$ given by $D^-(R|A) + D^-(R|B)$ where $D^-(R|T)$ is the one way distillable entanglement with classical communication from R to T only. Another provable lower bound is $\max_{\Lambda} [S(AV) - S(BV)]$ where the maximization is over channels $\Lambda : R \rightarrow V$. Strangely, $S(A|B) + S(B|A)$, the minimum rate for Alice to send her state to Bob, plus the minimum rate for Bob to send to Alice is not a lower bound, and we give examples of states for which $S(A|B)$ [or $S(B|A)$] can be very large while the rate for state exchange is small.

As with Schumacher compression, we consider the case of sources producing unknown states, and we know the statistics of the source only through the density matrix (extension to the case of unknown sources is also possible [14]), but we make no assumptions about the ensemble of states which may be emitted by the source – the states are unknown. We consider two separated parties, in possession of n copies of state ρ_{AB} . A faithful protocol is one which works with high probability, averaged over all possible unknown states in an ensemble. An elegant reformulation of this is to consider a reference system R , and total pure state $|\psi\rangle_{ABR}$, and define success of the protocols by demanding that after Alice's state has been transferred to Bob's site, the total state $|\psi\rangle_{ABR}$ should be virtually unchanged. More formally:

Definition 1 A *faithful state merging protocol* from

Alice to Bob is an operation that transforms the state $\psi_{ABR}^{\otimes n}$ into state $\rho_{ABB'B''R}^{merg}$ such that for large n

$$F(\rho_{ABB'B''R}^{merg}, \phi_{AB} \otimes \psi_{B'B''R}^{\otimes n}) \rightarrow 1 \quad (1)$$

where $\psi_{B'B''R}$ is equal to the original state ψ_{ABR} if we substitute $A \rightarrow B'$ and $B \rightarrow B''$, and the state ϕ_{AB} is arbitrary. The fidelity $F(\rho, \sigma) = \text{Tr}(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}})$, and subsystems B, B', B'' are at Bob's site. Allowing classical communication for free, the **partial information** is the rate amount of pure entanglement needed to achieve state merging (taking into account the entanglement left behind in the form of ϕ_{AB}).

Typically, the state ϕ_{AB} will be the possible distilled pure entanglement which might be gained after the protocol. Similarly,

Definition 2 A faithful state exchange protocol between Alice to Bob is an operation that transforms the state $\psi_{ABR}^{\otimes n}$ into state ρ_{ABR}^{ex} such that for large n

$$F(\rho_{ABR}^{ex}, \psi_{BAR}^{\otimes n}) \rightarrow 1 \quad (2)$$

where ψ_{BAR} is equal to the original state ψ_{ABR} if we exchange A with B (i.e. perform the swap operation). Allowing classical communication for free, the **uncommon information** $\Upsilon(A : B)$ is the minimum rate of pure entanglement required to achieve state exchange.

State exchange for the completely mixed density matrix is equivalent to the swap operation and it was shown that two bits of pure entanglement are necessary and sufficient to perform swap on two qubits [15, 16]. However, we will now see that if some correlations exist between the two systems, and we have many copies of the state, we can actually do better. We first look at upper bounds for $\Upsilon(A : B)$, based on specific protocols for state exchange:

Merge-and-send protocol: Alice merges her state with Bob at a cost of $S(A|B)$, who then sends his state to Alice at a cost of $S(B)$. The total rate R_{ms} is thus $S(AB)$. Here we see how the no-cloning theorem enters into the situation. Alice is able to merge her state with Bob's, taking advantage of the fact that he has some prior information (the state ρ_B). She thus sends her state at the lowest possible rate. However, once she has sent her state, she is left with nothing (unlike in the classical case where she can make a clone of her message), and Bob must send at the maximum rate of $S(B)$. Since individually, each party's partial information can be negative, it is the no-cloning theorem which prevents the rate of state exchange from being negative.

Double-copy protocol: Each party coherently copies their state to an ancilla: $A \rightarrow A'A''$, $B \rightarrow B'B''$ in some known basis which gets optimized. I.e. Alice applies the operation $|a\rangle_A |0\rangle_{A'} |0\rangle_{A''} \rightarrow |0\rangle_A |a\rangle_{A'} |a\rangle_{A''}$ for some basis a , and similarly Bob performs this operation in some basis b of his choice. Then:

1. Alice merges one of her copies of her state to Bob at a cost of $S(A'|B)$
2. Bob merges one of his copies with Alice at a cost of $S(B'|A'')$
3. Alice merges her second copy with Bob at a cost of $S(A''|A'B'')$
4. Bob merges his second copy with Alice, costing $S(B''|B')$

The total cost gives the following achievable rate R_{dc} for this protocol

$$\begin{aligned} R_{dc} &= \min_{ab} (S(A'B) + S(AB') - S(A') - S(B')) \quad (3) \\ &= \min_{ab} \left(\sum_a p_a S(\sigma_B^a) + \sum_b p_b S(\sigma_A^b) \right) \\ &= E_f(A : R) + E_f(B : R) \quad (4) \end{aligned}$$

where the minimization is taken over bases a, b , and E_f is the entanglement of formation [12]; regularisation (optimising over many copies of input state) leads to the better upper bound by the sum of the entanglement costs [13]. The states σ_A^b (σ_B^a) are those that would be induced on A (B) after a measurement on B (A) with outcomes b (a) and probabilities p_b (p_a). The measurement basis is the same as the basis $|a\rangle$ and $|b\rangle$ chosen in the initial copying step. The second equality of Equation (4), just comes from the fact that $S(A')$ and $S(B')$ are the same as the classical entropy $H(\{p_a\})$ and $H(\{p_b\})$. The third equality comes from the fact that a measurement on system A which minimizes the entropy of system B (conditioned on the outcomes of measurements), can alternatively be thought of as a measurement which produces pure states $|\psi^a\rangle_{BR}$ – i.e. it is a decomposition of ρ_{BR} into pure states $|\psi^a\rangle_{BR}$ with minimal total entanglement.

Expression (3) can also be interpreted as the sum of two classical-quantum conditional entropies, each of the form

$$SH(A|B) \equiv \inf_{\Lambda} (S(A\Lambda(B)) - S(\Lambda(B))). \quad (5)$$

I.e., conditional entropies obtained after applying the decohering map Λ on the conditioning system as is done in the protocol.

Note also that we can express this rate [17] in terms of a measurement of classical correlations, the Henderson-Vedral quantity [18] which we regularize C_{HV}^{∞}

$$R_{dc} = S(A) + S(B) - C_{HV}^{\infty}(A|B) - C_{HV}^{\infty}(B|A). \quad (6)$$

C_{HV}^{∞} is operationally equal to the one-way distillable common randomness [19]. Given that we have here a very simple protocol involving only four rounds, it seems possible that a more complicated protocol with many rounds

may be related not to C_{HV}^∞ but perhaps the classical information deficit Δ_{cl} [10].

Modified double copy protocol: One can modify the preceding protocol slightly, by not required the two parties to perform a complete copying operation. Each can divide their states into parts which are copied, and parts which are merged. We will see that this can be better.

The double copy protocol is optimal for the so-called classical states, i.e. states of the form

$$\varrho_{AB}^{cl} = \sum p_{ab} |a\rangle\langle a| \otimes |b\rangle\langle b| \quad (7)$$

since for these states one can copy in the local eigenbasis without changing any of the entropies. One can thus achieve a rate of $S(A|B) + S(B|A)$ which is optimal due to the lower bound of Theorem 2 proven below. The modified double copy protocol appears to be optimal for one-sided classical states, for example those of the form

$$\varrho_{AB}^{cl} = \sum p_a |a\rangle\langle a| \otimes \sigma_B^a \quad (8)$$

with the classical part on Alice's side. In this case, Alice copies and merges one of her copies with Bob who then merges his entire state with Alice's second copy. Alice then merges this second copy, again achieving the rate of $S(A|B) + S(B|A)$. That $S(B|A)$ qubits need to be sent from Bob follows from Theorem 2 proven below and we suspect that $S(A|B)$ bits also needs to be sent from Alice.

We finally mention another protocol: **do nothing**. This is possible (and clearly optimal) for states which are supported on only the symmetric (or antisymmetric) subspace of Alice and Bob, or are locally equivalent to such states. For symmetric or antisymmetric states on AB , $|\psi\rangle_{ABR} = \pm |\psi\rangle_{BAR}$, and thus nothing needs to be done since a global phase does not influence the three-party density operator. In particular, all pure states on AB have $\Upsilon(A : B) = 0$, as one would expect: they are fully correlated in the Schmidt basis, and thus contain no uncommon information. Surprisingly, neither $S(A|B)$ nor $S(B|A)$ are zero for such (anti-)symmetric states, thus if the task is for Alice to send her state to Bob, she needs $S(A|B)$ bits of entanglement, while if we demand that they perform the additinal task of Bob sending his state to Alice, the task becomes easier, and no quantum or classical communication needs to be exchanged. In the classical case, this of course never happens.

By exhibiting particular protocols, we thus obtain

Theorem 1 *The uncommon information $\Upsilon(A : B)$ is upper-bounded $\Upsilon(A : B) \leq S(AB)$ and $\Upsilon(A : B) \leq E_c(A : R) + E_c(B : R)$.*

We now turn to lower bounds, and will prove

Theorem 2 *The uncommon information $\Upsilon(A : B)$ satisfies the following lower bounds:*

$$\begin{aligned} \Upsilon(A : B) &\geq D^\rightarrow(R)A + D^\rightarrow(R)B \text{ and} \\ \Upsilon(A : B) &\geq \max_{\Lambda} [S(BV) - S(AV)], \end{aligned}$$

where the maximization is over channels $\Lambda : R \longrightarrow V$.

The proof of Theorem 2 is straightforward – for the first inequality, we imagine R as a referee who will check to see whether the output state ρ_{ABR}^{ex} is close in fidelity to $|\psi\rangle_{ABR}$. Before Alice and Bob begin the protocol, the referee performs one way distillation with Alice or Bob by performing local operations on her state. To distill maximally entangled states she would normally communicate with the other party, but this isn't necessary – it is only used to tell Alice or Bob which parts of their state contain the distilled entanglement. From the referee's perspective she holds $D^\rightarrow(R)A$ (or $D^\rightarrow(R)B$) bits of pure entanglement with A (or B). Imagine she distills entanglement (i.e. state ψ^+) with Alice. Then clearly ψ^+ on RA must be transferred by Alice to Bob, since the referee can check after completion of the protocol by asking Bob for the appropriate bits, and checking the fidelity of the subsystem of ρ_{ABR}^{ex} which contains ψ^+ . However, Alice and Bob perform their protocol before they know which party the referee distilled with, and thus from their point of view, pure state entanglement with R may exist on both their states which needs to be transferred to the other party. Thus just as Alice needs to transfer $D^\rightarrow(R)A$ to Bob, Bob also needs to transfer $D^\rightarrow(R)B$ qubits to Alice in case the referee distilled entanglement with him.

The second inequality comes by imagining dividing R into two parts, E and V (which is equivalent to a channel with E treated as the channel's environment), and giving ρ_V to Alice and ρ_E to Bob. Before the protocol, the entanglement is $S(AV)$ and after the state exchange the entanglement is $S(BV)$. Since entanglement cannot increase more than the number of qubits exchanged, the difference between final and initial entanglement is a lower bound on the number of sent qubits. Optimizing over splittings of ρ_R gives the required bound. \square

Let us turn from uncommon information to the notion of common information (which can be taken as a more general notion than mutual information [9]). State exchange considerations suggest that it be given by $\mathcal{C}(A : B) \equiv S(AB) - \Upsilon(A : B)$, i.e. the uncommon information subtracted from the total information. Such a quantity is always positive by Theorem 1, but is very different from the mutual information (for example, it is zero for pure states). Part of the reason for this is that mutual information measures the correlations between the two parties, while the common information quantifies how much information *about a reference system* the two parties share in common. It is thus zero for pure

states because a pure state has no information about the reference system, while it is maximal for the symmetric states, where all the information is common. It would be interesting to explore this notion of common information further, especially compared with other notions such as the mutual information, coherent information, distillable entanglement and entanglement of formation.

We thank Charlie Bennett for suggesting the nickname for the uncommon information. JO acknowledges the support of the Royal Society, the Newton Trust, and EU grant PROSECCO (IST-2001-39227). AW was supported by EU grant RESQ (IST-2001-37559), the U.K. Engineering and Physical Sciences Research Council's "QIP IRC", and a University of Bristol Research Fellowship.

-
- [1] C. Shannon, *Bell Syst. Tech. J.* **27**, 379 (1948).
 - [2] B. Schumacher, *Phys. Rev. A* **51**, 2738 (1995).
 - [3] D. Slepian and J. Wolf, *IEEE Trans. Inf. Theory* **19**, 461 (1971).
 - [4] M. Horodecki, J. Oppenheim, and A. Winter, *Nature* **436**, 673 (2005), quant-ph/0505062.
 - [5] M. Horodecki, J. Oppenheim, and A. Winter, quant-ph/0512247, to appear in *Comm. Math. Phys.*
 - [6] A. Wehrl, *Rev. Mod. Phys.* **50**, 221 (1978).
 - [7] R. Horodecki and P. Horodecki, *Phys. Lett. A* **194**, 147 (1994).
 - [8] N. Cerf and C. Adami, *Phys. Rev. Lett* **79**, 5194 (1997), quant-ph/9512022.
 - [9] Other notions of what it means for two variables to share information also exist e.g. A. D. Wyner, *IEEE Trans. Inf. Theory*, 21, 163 (1975).
 - [10] J. Oppenheim, K. Horodecki, M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. A* **68**, 022307 (2003), quant-ph/0207025.
 - [11] M. Horodecki and R. Horodecki, *Phys. Lett. A* **244**, 473 (1998), quant-ph/9705003.
 - [12] C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1997), quant-ph/9604024.
 - [13] P. Hayden, M. Horodecki, and B. Terhal, *J. Phys. A* **34**, 6891 (2001), quant-ph/0008134.
 - [14] R. Jozsa, M. Horodecki, P. Horodecki, and R. Horodecki, *PRL* **81**, 1714 (1998), quant-ph/9805017.
 - [15] J. Eisert, K. Jacobs, P. Papadopoulos, and M. Plenio, *Phys. Rev. A* **62**, 052317 (2000).
 - [16] D. Collins, N. Linden, and S. Popescu, *Phys. Rev. A* **64**, 032302 (2001), quant-ph/0005102.
 - [17] M. Koashi and A. Winter (2003), quant-ph/0310037.
 - [18] L. Henderson and V. Vedral, *J. Phys. A* **34**, 6899 (2001), quant-ph/0105028.
 - [19] I. Devetak and A. Winter, quant-ph/0304196.